学校编码：10384　　分类号_____

学号：X2005223003　　UDC _____

厦门大学

硕 士 学 位 论 文

# 基于身份的代理盲签名体制的研究

# Research on ID-based Proxy Blind Signature Scheme

农强

指导教师姓名：吴顺祥 教授

陈宝兴 教授

专 业 名 称：控制理论与控制工程

论文提交日期：2008 年 4 月

论文答辩时间：2008 年 6 月

学位授予日期：　　年　月

答辩委员会主席：_____

评　　阅　　人：_____

2008 年 4 月

# 厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　　月　　日

# 厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其它指定机构送交论文的纸质版和电子版，有权将学位论文用于非营利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适应本规定。

本学位论文属于

1、保密（　），在　　年解密后适用本授权书。

2、不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　月　日

导师签名：　　日期：　　年　月　日

# 摘　要

信息安全是信息社会急需解决的最重要问题之一，它已成为信息科学领域的一个重要的新兴学科。数字签名技术是提供认证性、完整性和不可否认性的重要技术，因而是信息安全的核心技术之一。随着对数字签名研究的不断深入，随着电子商务、电子政务的快速发展，简单模拟手写签名的一般数字签名已不能完全满足需要，研究具有特殊性质的数字签名成为数字签名的主要研究方向。

本文的主要内容是代理盲签名方案的研究。代理盲签名作为一种新型的数字签名方案，首先是由 Lin 等人在 2000 年提出。代理盲签名兼具了代理签名和盲签名的优点，正是这一特性，使得代理盲签名可以应用到电子商务、电子货币等应用领域，具有很高的实际应用价值。

基于身份的密码系统解决了传统公钥体制中利用公钥基础设施来管理公钥证书的复杂性和成本过高的问题，可与公钥证书基础设施密码体制形成牢固有利的互补。近几年，双线性配对已经广泛应用于密码学，它已经成为构建基于身份的密码体系的基本工具。尽管基于身份的签名方案具有签名长度短的优点，但是由于双线性配对运算非常耗时，降低了方案的效率，限制了基于身份的方案在实际中的应用。

围绕着目前基于身份的代理盲签名方案的安全性和效率问题以及其密钥托管问题，本文所做的工作主要有：

1)．对现有的几个基于身份的代理盲签名方案进行了安全性分析，指出李方案存在安全性问题，如原始签名人的伪造攻击问题，代理签名权力的滥用问题以及代理签名人事后可以追踪签名等。

2)．针对李方案的安全性漏洞，提出了一个改进的代理盲签名方案。并对新方案与原方案进行了对比安全性分析，证明了新的代理盲签名方案可以抵抗原始签名人的伪造攻击，并有效的克服了原方案中的不足。

3)．针对目前基于身份的签名体制中的密钥管理问题，提出了一个基于身份的新型代理盲签名方案，消除了私钥产生机构 PKG ( Private Key Generator )能够任意伪造用户签名的安全隐患，分析表明，该方案不仅能满足代理盲签名所要求的各种性质，而且效率也优于已有文献。

**关键词**：数字签名；基于身份；代理盲签名；私钥产生机构

## Abstract

Information security is one of the most important problems in modern information society and becomes a new important subject in the information science. Digital signature, which can prove authentication, integrity and non-repudiation, is one of the key techniques of information security. As the deepening of digital signature research and the rapid development of E-commerce and E-governance, the standard signature, which is a simple simulacrum of handwritten signature, can not still meet the need in practice, thus making research on the digital signatures with additional properties becomes a main research direction in digital signature.

The main content of this paper is the research of proxy blind signature scheme. As a kind of new digital signature schemes, proxy blind signature is first proposed by Lin *et al.* in 2000. Proxy blind signature scheme has the characteristic of the proxy signature scheme and the blind signature scheme. So it can be applied in the field of electronic commerce and electronic cash etc.

In traditional public key infrastructure ( PKI ) system, managing public key certification causes problems of complexity and high cost. Fortunately, identity-based cryptography has solved these kinds of problems, and it is also a good replenisher to PKI system. In the last couple of years, the bilinear pairings has been applied to various applications in cryptography. They are basic tools for construction of identity-based cryptographic schemes. Although identity-based signature scheme has the advantage of short signature size, the time-consuming computation of the pairing lowers the efficiency of the scheme, thus restrict the application of identity-based signature.

The main work in this paper is to research on some problems about current identity-based proxy blind signature schemes. The main results are as follows:

1). Several existing identity -based proxy blind signature schemes are analyzed. This paper shows that the Li *et al.*'s scheme does not posses the unforgeability property. The original signer can forge a valid proxy blind signature for any message, and the proxy signer can misuse the signing capabilities. At the same time, the proxy signer can make a linkage between a signature and the corresponding message of signing protocol after signing.

2). An improved new identity-based proxy blind signature scheme is proposed based on the existing proxy blind signature schemes. The security of the new scheme is also discussed and shown that it can resolve the security problems existing in the original scheme.

3). To avoid the key escrow problem in identity-based signature scheme, a new identity-based proxy blind signature scheme without trusted private key generator (PKG) is proposed. Analysis shows that the proposed scheme can satisfy all the required properties of a proxy blind signature. Furthermore, its efficiency is also better than that of the existing ones.

**Key Words**: Digital signature; Identity-based; Proxy Blind Signature; Private Key Generator

# 目 录

# 第一章　绪论

## 1.1 数字签名研究背景及意义

计算机技术的高速发展为人类提供了高度的自动化和现代化，网络的迅猛发展为人们提供了便捷、快速的信息交流方式，使人类社会迅速进入了信息化时代。互联网的发展和壮大使得人们足不出户就可以洞晓天下人和事，极大的方便了人们的学习、工作和生活。现在，计算机应用已经渗透到政治、经济、军事、科学文化和家庭生活等社会的各个领域。然而，现代信息技术也是一把双刃剑，它给人们带来方便的同时，也带来了许多麻烦。由于信息的传递、存储、处理等过程往往是在开放的通信网络上进行的，而 Internet 从建立开始就缺乏安全方面的总体构想和设计，因而因特网的信息容易受到窃听、截取、修改、伪造、重放等各种攻击手段的威胁,其安全及其脆弱。据 Financial Times 曾做过的统计，平均每 20 分钟就有一个网络入侵发生，计算机犯罪已经成为现在普遍的国际性问题。计算机犯罪案的迅速增加，使各国的计算机系统、特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。我国的网络犯罪也成激增之势，网络犯罪已经渗透到社会生活的方方面面，随着计算机技术的进一步发展和应用，网络犯罪将更加严重。网络安全成为现在网络应用亟待的问题。网络安全包括物理安全、网络系统安全、数据安全、信息内容安全和信息基础设施安全等。网络安全是一项系统工程，要从法律、制度、管理和技术上采取综合措施，以便相互补充，达到较好的安全效果。管理是所有安全领域的重要组成部分，而技术措施则是最直接的屏障，目前常用而有效的网络安全技术主要有如下几种。

1). 加密：加密就是对信息进行一种变换，把可懂的信息变为不可理解的信息，在传输过程或存储时进行加密，使得信息变为不可懂的，这样即使攻击者得到这些信息也无法解读，从而保护信息的安全。

2).数字签名：数字签名提供了一种鉴别方法，它采用一种数据交换协议，使得接受者能够鉴别发送者的身份且发送者以后不能否认发送过该数据的事实。数字签名解决了伪造、抵赖、冒充和篡改等安全问题。

3). 鉴别：鉴别的目的是验明用户身份或信息内容本身，别的方法在网络环境中用的比较多的是数字签名技术。当然还有一些其他技术，如防火墙技术、入

侵检测技术等。

网络安全从本质上讲就是网络上的信息安全。信息安全是对信息的保密性、完整性和可用性的保护。数字签名技术是保障这种安全需要的一种重要手段，它可以保证信息完整、鉴别发送者身份真实性与不可否认性；利用数字签名本身的基础技术如加密技术，还可以保证信息机密性。数字签名具有与传统手写签名同样的法律效力，而且它不需要面对面就可以实现，可以不受地点的限制。数字签名技术是当前网络安全的研究热点之一，它使人们可以实现远距离的身份认证、密钥分配、电子交易等，已经被广泛地应用到电子商务、电子银行、电子政务等领域。

在日常生活中，使用手签名与印章随处可见，其目的是：证明签署双方已经签署该文件，从而该文件能得到法律的认证、核准，可以在法律上生效，签署双方必须履行该文件上规定的条款，签署双方不能反悔。而数字签名是手写签名电子对应物，数字签名是以公钥密码体制为基础的，在具体实施过程中，仅仅签名者自己掌握私钥，而只公开其对应的公钥，签名者用自己的私钥变换数据，其他人用签名者对应的公钥就可以对数据进行逆变换，而得到原始数据，因为只有对应的公钥才能变换出该私钥变换后的数据，从而可以鉴别该数据是谁进行的变换处理，即是谁的签名。它的主要功能是实现对电子形式存放的文件的认证。数字签名与传统的签名相比有许多特点：首先，在数字签名中签名同签名文件是分开的，需要一种方法将签名与签名文件绑定在一起，而在传统手写签名中，签名是被签名文件的一部分。其次，在签名验证的方法上，数字签名利用一种公开的方法对签名进行验证，任何人都可以对签名进行验证，而传统手写签名的验证是由经验丰富的文件接收者通过与以前的签名进行比较来确定的。最后，在数字签名中，有效签名的复制同样是有效的签名，而在传统的手写签名中，签名的复制是无效的。

数字签名能够有效地解决网络身份识别认证、网络授权、公文处理和法律证据等问题，应用前景广阔，受到了各国政府的广泛重视。作为重要的数字证据，美国、新加坡、日本、韩国、欧盟等电子商务开展的较早的国家和地区都相继通过法案赋予数字签名法律效力，中国全国人大也已于 2004 年 8 月通过了《中华人民共和国电子签名法》，该法对确定电子签名的法律效力、规范电子签名的行

为、明确电子服务机构的法律地位及电子签名的安全保障等多个方面作了具体规定，它适应了信息化发展的需要，也必将对我国电子商务、电子政务的发展起到极其重要的促进作用。数字签名具有认证性、完整性和不可否认性的特点使其在电子商务和电子政务系统中起着重要作用，反过来，电子商务和电子政务系统的快速发展又有力推动着数字签名技术不断向前发展。目前，数字签名技术已被广泛应用于电子支付、电子拍卖、电子投标、电子投票和电子彩票等协议中。随着对数字签名技术研究的深入以及实际应用的需要，普通的数字签名已不能满足人们的需要，研究数字签名，提高数字签名的安全性，提出各种具有特殊性质、特殊功能、能满足特定要求的特殊类型的签名方案，具有十分重要的理论意义和现实意义。因此多年来国内外学者提出了许多具有特殊性质或特殊功能的数字签名，如：

- 1982 年，Chaum 引入了盲签名(blind signature)[1]；
- Itakura 和 Nakamura 引入了多重签名(multi-signature)[2]；
- 1989 年，Chaum 引入了不可否认签名(undeniable signature)[3]；
- Even，Goldreieh 和 Mieali 引入了在线/离线签名(on-line/off-line digital signatures)[4]；
- Fiat 引入了批签名(batch signatures)[5]；
- De Soete 和 Vedder 引入了共享验证签名(shared verification signature)[6]；
- 1991 年，Desmedty 引入了门限签名(threshold signature)[7]；
- Chaum 和 Heyst 引入了群签名(group signature)[8]；
- Pfitzmann 和 Waidner 引入了失败停止签名(fail-stop signature)[9]；
- 1992 年，Goldwasser 引入了不变签名(invariant signatures)[10]；
- Lim 和 Lee 引入了有向签名(directed signature)[11]；
- Nyberg 和 Rueppel 引入的消息恢复签名(messgage recovery signature)[12,13]；
- 1994 年，Chaum 引入了指定证实人签名(designated comfirmer signature)[14]；
- 1996 年，Kim，Park 和 Won 引入了指名签名(nominative signature)[15]；

• Mambo，Usuda 和 Okamoto 引入了代理签名(proxy signature)[16]；

• 1997 年，Zheng 引入了签密(signcryption)[17]；

• Jakobasson 和 Yung 引入了魔术墨水签名(magic ink signatures)[18]；

• 2000 年，Rivest 引入了同态签名(homomorphic signature)和聚合签名(aggregate signature)[19]；

• Krawczyk 和 Rabin 引入了变色龙签名(chameleon signatures)[20]；

• 2001 年，Rivest，Shamir 和 Tauman 引入了环签名(ring signature)[21]；

• 2002 年，Micali 和 Rivest 引入了传递签名(transitive signature)[22]；

• Johnson，Molnar，Song 和 Wagner 引入了可编辑签名(redactable signature)[23]；

• Lee 和 Kim 引入了自证明签名(self-certified signature)[24]；

• 2003 年，Boneh，Gentry，Lynn 和 Shacham 引入了可验证加密签名(verifiably encrypted signature)[25]；

• 2004 年 L.Chen，C.Kudla，和 K.G.Paterson 引入了并发签名(concurrent signature)[26]；

这些签名体制还可以组合出更多的签名体制，如群盲签名(group blind signature)[27]、门限代理签名(threshold proxy signature)[28]、代理盲签名(proxy blind signature)[29]、代理多重签名(proxy multi-signature)[30]、盲门限签名(blind threshold signature)[31]等等。Z.Cao 在文献[32]中细致地分析了各种特殊签名，并组合了几乎全部的特殊功能的签名类型。有关数字签名的更多文献请参见[33,34]。

## 1.2 代理盲签名研究现状

不论是手写签名和印鉴，还是数字签名，都代表了签名人的一种权力。称之为签名人联合灌名权力( Polder of Siding )。在手写签名中，签名权力依赖于签名人的书写习惯和书法特征；在印鉴中，签名权力依赖于签名人掌握的印章；在数字签名中，签名权力依赖于签名人的秘密密钥。容易看出，印鉴和手写签名之间有一个主要区别：生成印鉴的印章可以在不同的用户之间方便地传递，只要是相同的一枚印章，则不论其使用者是谁，都可以生成相同的印鉴；而生成手写签名